

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Craig B. Gentry		
Title:	NTT DOCOMO INC.		
Patent No.:	7,657,748 B2	Date of Patent:	February 2, 2010
Serial No.:	10/521,741	Filing Date:	August 28, 2003
Examiner:	Hadi S. Armouche	Group Art Unit:	2432
Docket No.:	M-16094 US (70216.178)	Confirmation No.:	7038

San Jose, California
November 10, 2010

ATTN: Certificate of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION
OFFICE'S MISTAKE

Dear Sir:

The Patentee submits herewith Form PTO-1050 for the above-identified patent. This submission corrects clerical and typographical errors by the U.S. Patent and Trademark Office (the Office).

The errors by the Office are as follows:

Column 8, Line 34: delete "(PKB, SKB)"; insert --(PK_B, SK_B)--.

Column 8, Line 44: delete the word "params"; insert --*params*--.

Column 8, Line 45: delete the words "masks S"; insert --masks *s*--.

Column 8, Line 46: delete the word "ID"; insert --*ID*--.

Column 8, Line 50 & 51: delete the words "s, params and ID"; insert --*s, params and ID*--.

Column 8, Line 52: delete the word "ID"; insert --*ID*--.

Column 8, Line 54: delete the words "params, ID and M"; insert --*params, ID and M*--.

Column 8, Line 55: delete the words "C to recover M"; insert --*C to recover M*--.

Column 10, Line 61 & 62: delete " $\hat{e}(P, P)^{abc}$ if P, aP, bP, and cP are known, but a, b, and c are not";
insert -- $\hat{e}(P, P)^{abc}$ if P, aP, bP, and cP are known, but a, b, and c are not--.

Column 10, Line 64 & 65: delete " $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$ ";
insert -- $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$ --.

Column 10, Line 66 & 67: delete " $g = \hat{e}(P, P)$, then $g^{abc} = g^{ab}c$ where $g^{ab} = \hat{e}(aP, bP)$ and $g^c = \hat{e}(P, cP)$ ";
insert -- $g = \hat{e}(P, P)$, then $g^{abc} = (g^{ab})^c$ where $g^{ab} = \hat{e}(aP, bP)$ and $g^c = \hat{e}(P, cP)$ --.

Column 11, Line 48: delete " $C = [rP, M \oplus H_2(g')]$ ", where $g = \hat{e}(Q, P_B) \in G_2$;
 insert $--C = [rP, M \oplus H_2(g')]$, where $g = \hat{e}(Q, P_B) \in (s_B P, P'_B) \in G_2$ --

Column 12, Line 59: delete the word "params"; insert $--params--$.

Column 13, Line 39: delete the word "params"; insert $--params--$.

Column 13, Line 43: delete the word "Musing"; insert $--M$ using--

Column 15, Line 7: delete the word "sendery"; insert $--sender y--$

Column 15, Line 11: delete the word "sendery"; insert $--sender y--$

Column 15, Line 60: delete " $m-1+1$ "; insert $--m-l+1--$

Column 15, Line 66: delete " $1-1$ "; insert $--l-1--$

Column 16, Line 10: delete " $n-1+1$ "; insert $--n-l+1--$

Column 16, Line 17: delete " $1-1$ "; insert $--l-1--$

Column 16, Line 25: delete " $n-1$ "; insert $--n-l--$

Column 19, Line 37: delete "sendery"; insert $--sender y--$

Column 20, Line 19: delete " $U_i = rP_{zi}$ for $k+1 \leq i \leq n+1$ ";
 insert $--U_i = rP_{zi}$ for $l+1 \leq i \leq n+1--$

Column 24, Line 40: delete the word "params"; insert $--params--$.

Claim 80 line 8 (Column 38, Line 11): delete "key!recipient"; insert $--key/recipient--$.

Claim 80 line 21 (Column 38, Line 24): delete "key!private"; insert $--key/private--$.

The Patentee requests a Certificate of Correction or an otherwise corrected patent at the expense of the Office to correct the errors identified on Form PTO-1050 submitted herewith. No new matter has been added. No fee is believed to be required. If a fee is required, please charge Deposit Account 08-1394 for the required fee.

If any questions remain or anything further is required to correct this patent, please contact the undersigned at (408) 660-4120.

Respectfully submitted,

By: Michael Shenker

Dated: November 10, 2010

Michael Shenker
 Attorney for Applicant(s)
 Reg. No. 34,250

Haynes and Boone, LLP
 IP Section
 2323 Victory Avenue, Suite 700
 Dallas, Texas 75219
 Telephone: 408.660.4120
 Facsimile: 408.392.9262
 ipdocketing@haynesboone.com

**FILED VIA EFS
 CERTIFICATE OF TRANSMISSION**

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's EFS-Web electronic filing system on November 10, 2010.

Sheila Badon
 Sheila Badon

November 10, 2010
 Date